UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,785	01/04/2001	Clive Jones	537-1052	4133

23644 7590 09/01/2006

BARNES & THORNBURG LLP
P.O. BOX 2786
CHICAGO, IL 60690-2786

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/913,785	JONES ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-10,21 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-10,21 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 8-10, 21, and 22 are pending in this office action.

2. Applicant's arguments, filed July 12, 2006, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 8-10, 21, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker (U.S. Patent No. 5,946,355) in view of Bright et al. (U.S. Patent No. 4,893,339).

Regarding claim 8, Baker teaches an apparatus for generating digital audio data comprising:

- A source of digital audio signals (fig. 2, DATA IN), and
- A data encoding device having:
    - A serial data input (fig. 2, DATA IN and col. 3, line 15);
    - An encoded serial data output (fig. 2, ref. num 20 and col. 3, lines 15-19);

- A permutation unit which generates an initial plurality of encoding bits from the multiple bit random word (fig. 2, ref. num 12, mainly the LFSR); and
- An encoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and an updated encryption key comprising a plurality of updated encoded bits (fig. 2, ref. num 12, the encoded output bit is sent along to the transmission channel and the updated encryption key remains stored in the LFSR after being shifted and updated),
  - Wherein an initial bit input on the serial data input is encoded with an encryption key comprising the initial plurality of encoding bits output by the permutation unit and each subsequent input bit is encrypted using an updated key which is derived from previous values of the encryption key and of the input bit (fig. 2, ref. num 12, the LFSR receives input bits, shifts out an output bit and the contents of the LFSR contain an updated key for the next bit), and
  - Wherein over time the encoded output bit stream comprises substantially white noise (col. 4, lines 21-30).

Baker does not teach a random number generator which generates a stream of random bits and a transformation unit comprising means for storing a predetermined number of values of the random bit to derive a multiple bit random word.

Bright et al. teaches a random number generator which generates a stream of random bits and a transformation unit comprising means for storing a predetermined number of values of the random bit to derive a multiple bit random word (col. 10, lines 44-48).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a random number generator and a transformation unit which stores values of random bits, as taught by Bright et al., with the apparatus of Baker. It would have been obvious for such modifications because the randomly created initialization vector, which is loaded into the linear feedback shift register (LFSR) to give it an initial value, because the randomness provided in the initial filling of the LFSR gives a different encoding outcome each time the LFSR is loaded.

Regarding claim 9, official notice is taken that wherein the output at the output port is in SPDIF or AES/EBU format. Applicant admits, on page 1, lines 20-24 of the instant application, that SPDIF & AES/EBU are the common output methods for audio. Bright et al. teaches the data signal can be an audio signal. It would have been obvious to a skilled artisan to use the common output methods for outputting audio signals.

Regarding claim 10, the combination of Baker in view of Bright et al. teaches comprising a compact disc player (see col. 1, line 4 of Baker, a digital receiver involves a device that can interpret the digital signals, such as a disc player).

Regarding claim 21, Baker teaches an apparatus for reconstructing digital audio signals comprising:

- An input for receiving encoded digital audio signals (fig. 2, ref. num 31);
- A receiver for supplying the encoded digital audio signals to a decoding device (fig. 2, ref. num 30); and
- An output for the reconstructed digital audio signal (fig. 2, DATA OUT); and
- A decoding device comprising:
    - A serial data input (fig. 2, ref. num 31);
    - A permutation unit which generates an initial plurality of bits from the multiple bit random word (fig. 2, ref. num 40, mainly the LFSR); and
    - A decoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming a key, to derive a decoded output bit and an updated key comprising a plurality of updated bits (fig. 2, ref. num 40, the decoded output bit is sent out as DATA OUT and the updated key remains stored in the LFSR after being shifted and updated),
    - Wherein an initial bit input on the serial data input is decoded with a key comprising the initial plurality of bits output by the permutation unit and each subsequent input bit is decrypted using an updated key which is derived from previous values of the key and of the input bit (fig. 2, ref. num 40, the LFSR receives input bits, shifts out an output bit and the contents of the LFSR contain an updated key for the next bit).

Baker does not teach a transformation unit comprising means for storing a predetermined number of values of random bits to derive a multiple bit random word.

Bright et al. teaches a transformation unit comprising means for storing a predetermined number of values of random bits to derive a multiple bit random word (col. 10, lines 44-48).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a transformation unit for storing values of random bits, as taught by Bright et al., with the apparatus of Baker. It would have been obvious for such modifications because the randomly created initialization vector, which is loaded into the linear feedback shift register (LFSR) to give it an initial value, because the randomness provided in the initial filling of the LFSR gives a different encoding outcome each time the LFSR is loaded.

Regarding claim 22, the combination of Baker in view of Bright et al. teaches a data communication system comprising all the limitations stated in the claim because the encoding and decoding are mirror processes of one another; the limitations of the encoding device are taught with reference to claim 8, and the limitations of the decoding device are taught with reference to claim 21.

Response to Arguments

5. Applicant argues that Baker does not teach combining each bit on the serial data input with a plurality of additional bits forming an encryption key (page 2).

Regarding applicant's argument, examiner disagrees with applicant. The LFSR (figure 2, reference number 12) represents, at any given time, the current encryption key. It gets updated by feeding through bits from the serial input data. The single bit inputted from the serial data input line is combined with a plurality of additional coding bits, those additional coding bits being part of the LFSR, which makes up the encryption key. After feeding through a certain number of bits from the serial data input, a single bit is outputted further down the line, while the LFSR contains several bits making up an updated encryption key (the key is updated because the LFSR has been 'clocked' several times by the feeding of single serial data input bits).

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brandon Hoffman

BH

NASSER MOAZZAMI
PRIMARY EXAMINER

8/31/06